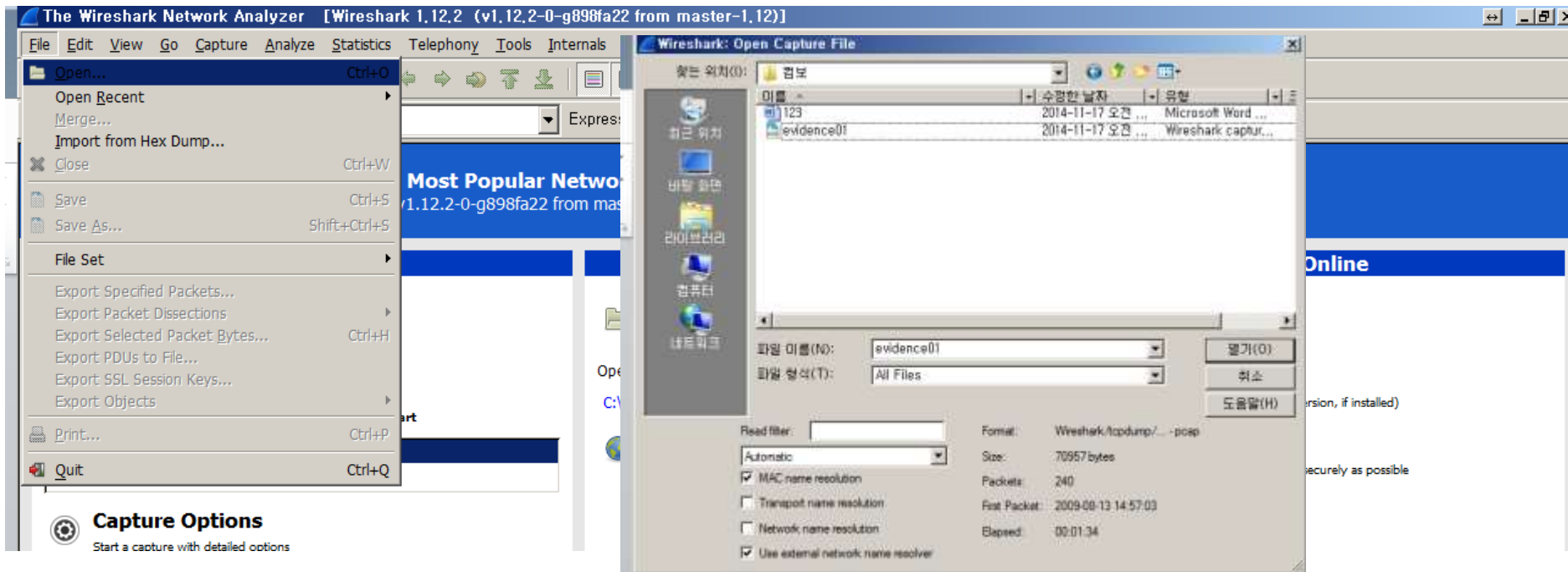


보안실습 8

[네트워크 트래픽에서 파일 추출하기]

준비물: Wireshark, evidence04.pcap, HexaEdit(Winhex)

트래픽 캡처 파일 열기 (evidence04.pcap)



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Conversation] 기능을 통해 호스트간의 트래픽 확인

Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

Summary
Comments Summary
Show address resolution
Protocol Hierarchy

Conversations

Endpoints
Packet Lengths...
IO Graph

Conversation List
Endpoint List
Service Response Time

29West
ANCP
BACnet
Collectd...
Compare...
Flow Graph...
HART-IP
HTTP
ONC-RPC Programs
Sametime
TCP StreamGraph
UDP Multicast Stream
WLAN Traffic

IP Statistics
BOOTP-DHCP...

103 59.597830 192.168.1.157
104 59.598074 192.168.1.157
105 59.598268 192.168.1.157
106 59.598613 192.168.1.157
107 61.051425 Dell_4d:4f:ae
108 61.051429 Hewlett-45:a
109 61.052925 192.168.1.159
110 61.052930 192.168.1.158
111 61.054660 192.168.1.159
112 61.054884 192.168.1.158
113 61.064823 192.168.1.159
114 61.065468 64.12.25.91
115 61.144314 192.168.1.159
116 61.144758 64.12.25.91
117 61.155756 192.168.1.159
118 61.155760 192.168.1.158
119 61.270615 192.168.1.158
120 61.270620 192.168.1.158
121 61.270623 192.168.1.159
122 61.270628 192.168.1.158
123 61.270632 192.168.1.158
124 61.270635 192.168.1.158
125 61.270638 192.168.1.159
126 61.270641 192.168.1.158
127 61.270644 192.168.1.158
128 61.270647 192.168.1.158
129 61.270651 192.168.1.158
130 61.270655 192.168.1.159
131 61.270658 192.168.1.158

Conversations: evidence01.pcap

Ethernet: 11 Fibre Channel FDDI IPv4: 14 IPv6 IPX JXTA NCP RSVP SCTP TCP: 7 Token Ring UDP: 9 USB WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel Start	Duration	bps A→B	bps B→A
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000000	94.3298	20.86	
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114000	0.0663	32819.52	246
192.168.1.158	51128	64.12.24.50	443	40	4303	20	1681	20	2622	18.870898000	72.1626	186.36	
192.168.1.159	1221	64.12.25.91	443	40	6005	16	1799	24	4206	34.025532000	57.0382	252.32	
192.168.1.159	1271	205.188.13.12	443	47	31168	16	1451	31	29717	34.211454000	1.2039	9642.08	197
192.168.1.158	5190	192.168.1.159	1272	24	14142	15	13100	9	1042	61.052925000	0.2848	367918.10	292
192.168.1.159	1273	64.236.68.246	80	10	3509	5	1964	5	1545	93.356969000	0.3618	43422.99	34

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph B→A Close

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Conversation] 기능을 통해 호스트간의 트래픽 확인

Conversations: evidence01.pcap

Ethernet: 11 | Fibre Channel | FDDI | IPv4: 14 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | **TCP: 7** | Token Ring | UDP: 9 | USB | WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000000	94.3298	20.86	
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114000	0.0663	32819.52	248
192.168.1.158	51128	64.12.24.50	443	40	4 303	20	1 681	20	2 622	18.870898000	72.1626	186.36	2
192.168.1.159	1221	64.12.25.91	443	40	6 005	16	1 799	24	4 206	34.025532000	57.0382	252.32	5
192.168.1.159	1271	205.188.13.12	443	47	31 168	16	1 451	31	29 717	34.211454000	1.2039	9642.08	1974
192.168.1.158	5190	192.168.1.159	1272	24	14 142	15	13 100	9	1 042	61.052925000	0.2848	367918.10	293
192.168.1.159	1273	64.236.68.246	80	10	3 509	5	1 964	5	1 545	93.356969000	0.3618	43422.99	34

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph A←B Close

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Conversation] 기능을 통해 호스트간의 트래픽 확인

Conversations: evidence01.pcap

Ethernet: 11 | Fibre Channel | FDDI | IPv4: 14 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | **TCP: 7** | Token Ring | UDP: 9 | USB | WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000000	94.3298	20.86	
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114000	0.0663	32819.52	248
192.168.1.158	51128	64.12.24.50	443	40	4 303	20	1 681	20	2 622	18.870898000	72.1626	186.36	2
192.168.1.159	1221	64.12.25.91	443	40	6 005	16	1 799	24	4 206	34.025532000	57.0382	252.32	5
192.168.1.159	1271	205.188.13.12	443	47	31 168	16	1 451	31	29 717	34.211454000	1.2039	9642.08	1974
192.168.1.158	5190	192.168.1.159	1272	24	14 142	15	13 100	9	1 042	61.052925000	0.2848	367918.10	293
192.168.1.159	1273	64.236.68.246	80	10	3 509	5	1 964	5	1 545	93.356969000	0.3618	43422.99	34

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph A←B Close

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

통신 내역 확인

Conversations: evidence01.pcap

Ethernet: 11 | Fibre Channel | FDDI | IPv4: 14 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 7 | Token Ring | UDP: 9 | USB | WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000000	94.3298	20.86	
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114000	0.0663	32819.52	248
192.168.1.158	51128	64.12.24.50	443	40	4 303	20	1 681	20	2 622	18.870898000	72.1626	186.36	
192.168.1.159	1221	64.12.25.91	443	40	6 005	16	1 799	24	4 206	34.025532000	57.0382	252.32	
192.168.1.159	1271	205.188.13.12	443	47	31 168	16	1 451	31	29 717	34.211454000	1.2039	9642.08	197
192.168.1.158	5190	192.168.1.159	1272	24	14 142	15	12 100	9	1 042	0.000000000	0.0049	367918.10	298
192.168.1.159	1273	64.236.68.246	80	10	3 509							43422.99	34

Apply as Filter
 Prepare a Filter
 Find Packet
 Colorize Conversation

Selected
 Not Selected
 ... and Selected
 ... or Selected
 ... and not Selected
 ... or not Selected

A ↔ B
 A → B
 A ← B
 A ↔ Any
 A → Any
 A ← Any
 Any ↔ B
 Any ← B
 Any → B

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph A←B Close

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Follow TCP Stream] 기능을 이용한 트래픽 확인

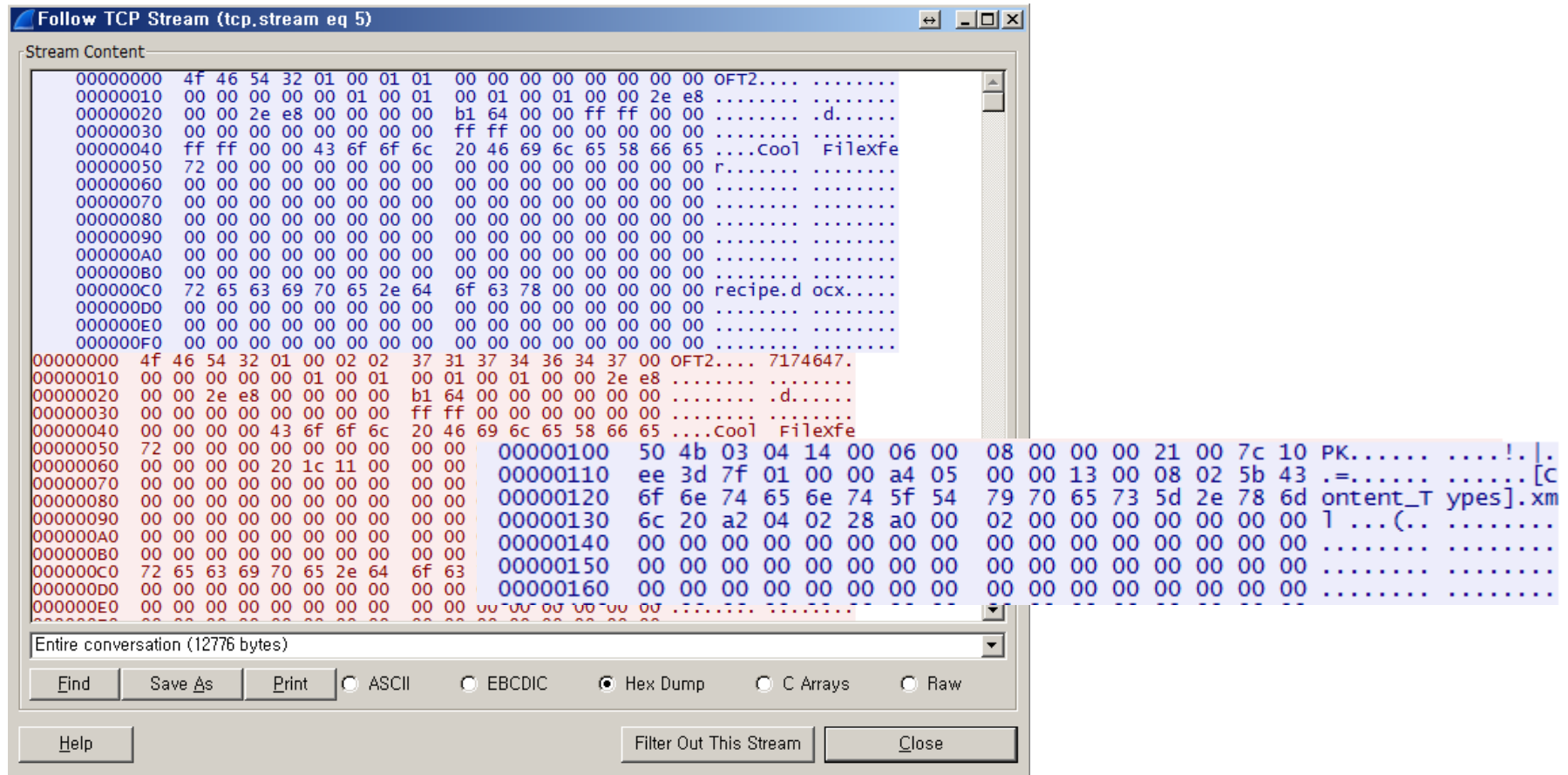
The image displays the Wireshark network protocol analyzer interface. The main window shows a packet capture from 'evidence01.pcap' using Wireshark 1.12.2. A filter 'tcp.stream eq 5' is applied. The packet list shows a series of packets between 192.168.1.158 and 192.168.1.159. A right-click context menu is open over packet 138, with 'Follow TCP Stream' selected. To the right, the 'Follow TCP Stream (tcp.stream eq 5)' window is open, displaying the raw data of the selected stream. The data appears to be a document, with visible text including 'recipe.docx' and 'Filexfe'. The bottom of the window shows options for displaying the data: ASCII, EBCDIC, Hex Dump, C Arrays, and Raw (selected).

No.	Time	Source	Destination	Protocol	Length	Info
109	61.052925	192.168.1.159	192.168.1.158	TCP	62	1272-5190 [SYN]
110	61.052930	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
111	61.054660	192.168.1.159	192.168.1.158	TCP	60	1272-5190 [ACK]
112	61.054884	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
117	61.155756	192.168.1.159	192.168.1.158	TCP	60	1272-5190 [ACK]
118	61.155760	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
119	61.270615	192.168.1.158	192.168.1.159	TCP	60	1272-5190 [ACK]
120	61.270620	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
121	61.270623	192.168.1.159	192.168.1.158	TCP	60	1272-5190 [ACK]
122	61.270628	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
123	61.270632	192.168.1.158	192.168.1.159	TCP	60	1272-5190 [ACK]
124	61.270635	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
125	61.270638	192.168.1.159	192.168.1.158	TCP	60	1272-5190 [ACK]
126	61.270641	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
127	61.270644	192.168.1.158	192.168.1.159	TCP	60	1272-5190 [ACK]
128	61.270647	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
129	61.270651	192.168.1.158	192.168.1.159	TCP	60	1272-5190 [ACK]
130	61.270655	192.168.1.159	192.168.1.158	TCP	60	5190-1272 [ACK]
131	61.270658	192.168.1.158	192.168.1.159	TCP	60	1272-5190 [ACK]
132	61.270662	192.168.1.159	192.168.1.158	TCP	60	5190-1272 [ACK]
133	61.270706	192.168.1.159	192.168.1.158	TCP	60	1272-5190 [ACK]
134	61.270711	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]
138	61.296969	192.168.1.159	192.168.1.158	TCP	60	1272-5190 [ACK]
139	61.337771	192.168.1.158	192.168.1.159	TCP	60	5190-1272 [ACK]

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Hex Dump]로 포맷을 변경 -> PK.. 확인 (매직넘버)



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Hex Dump]로 포맷을 변경 -> PK.. 확인 (매직넘버)

```
00000100  50 4b 03 04 14 00 06 00 08 00 00 00 21 00 7c 10 PK.....!.|.
00000110  ee 3d 7f 01 00 00 a4 05 00 00 13 00 08 02 5b 43 .=.....[C
00000120  6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d ontent_T ypes].xm
00000130  6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 1 ...(.
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

검색페이지에서 PK의 16진수 값 뒤에 함께 오는 값을 검색해 보면,
OFFICE 계열의 포맷이라는 것을 확인할 수가 있다.

50 4B 03 04 14 00 06 00

DOCX, PPTX, XLSX

PK.....

Microsoft Office Open XML Format (OOXML) Document

NOTE: There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively.

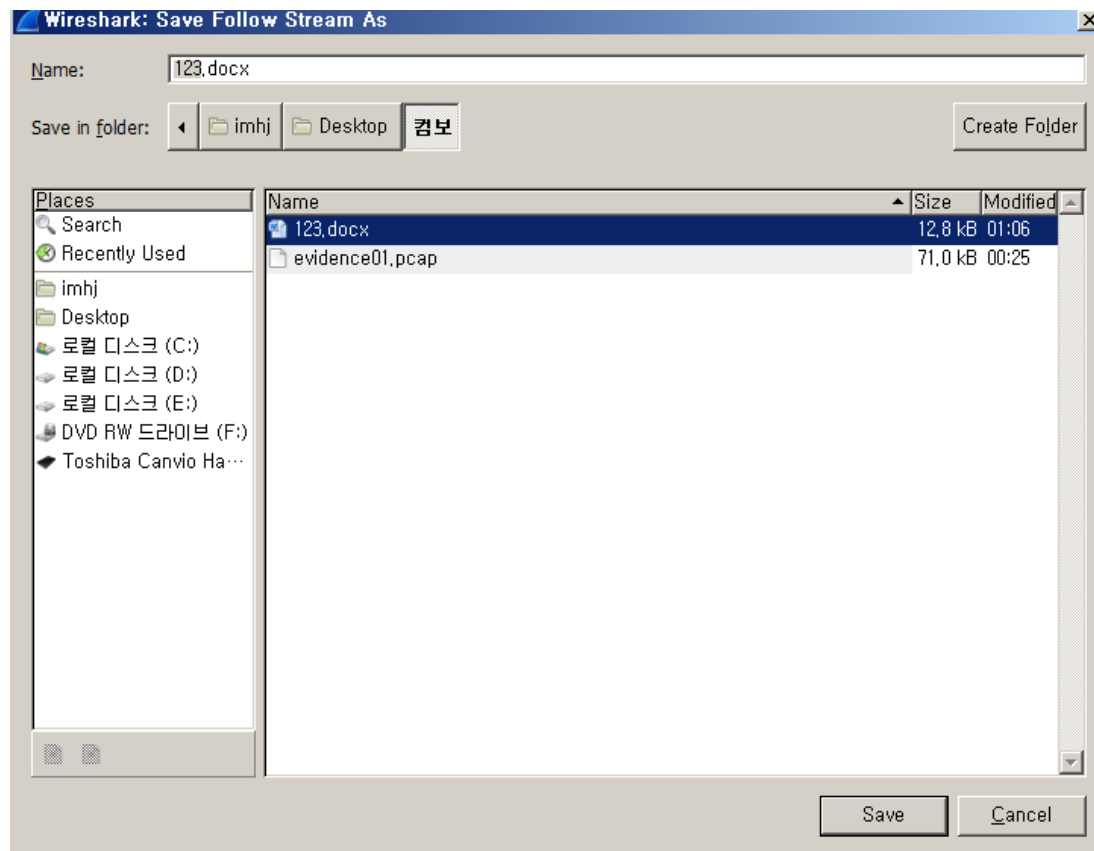
Trailer: Look for 50 4B 05 06 (PK..) followed by 18 additional bytes at the end of the file.

이로써 해당 블록이 OFT2 블록에서 보였던 recipe.docx라고 가정하고 접근해 볼 수 있다.

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Hex Dump]로 포맷을 변경 -> PK.. 확인 (매직넘버)



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

Winhex를 통해 필요없는 부분 자르기

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.